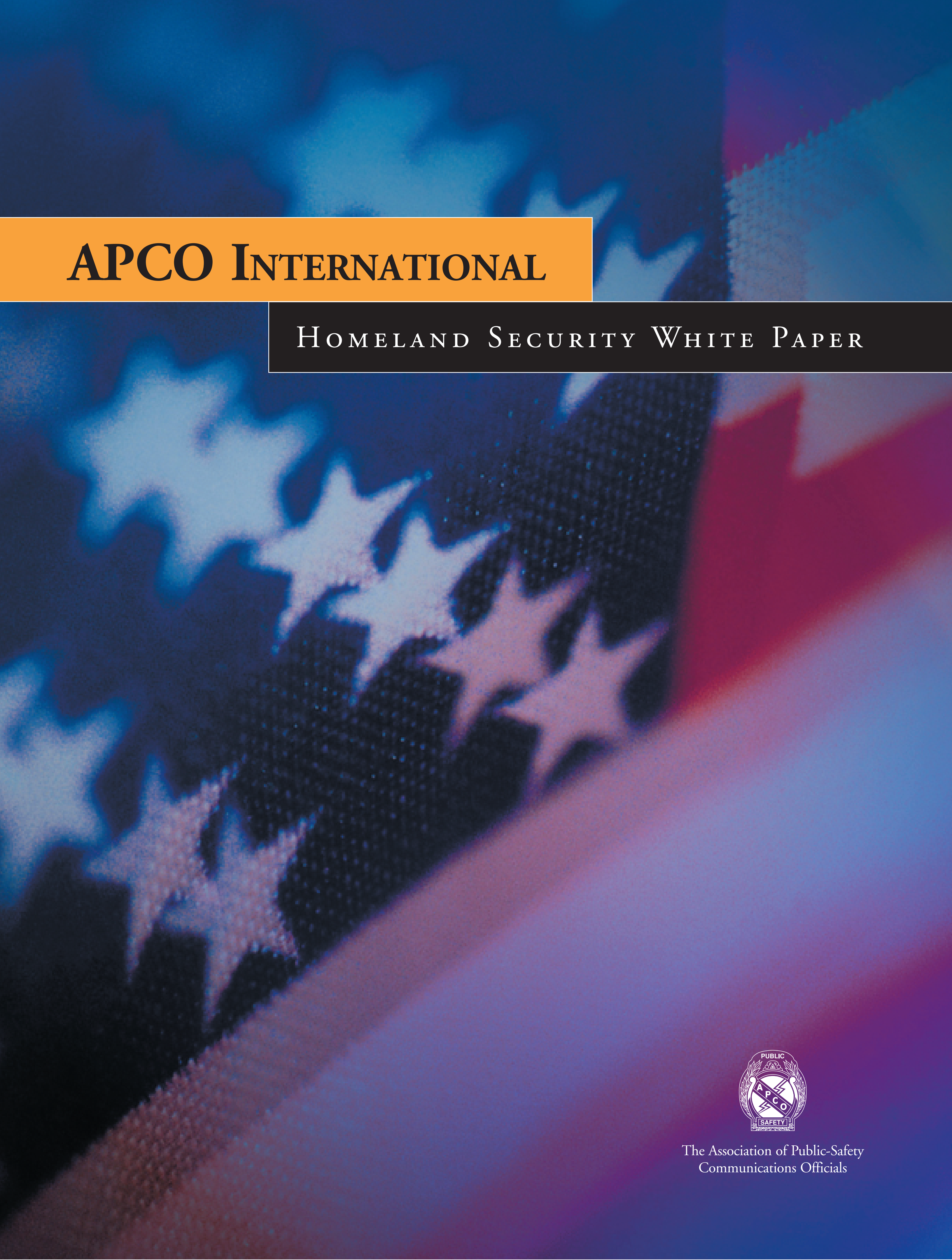


APCO International

Homeland Security White Paper

The Association of Public-Safety
Communications Officials

APCO Homeland Security Task Force

Gregory S. Ballentine, *Liaison to the Board*
First Vice President, MARC
Kansas City, Missouri

William A. Cade, Jr.
Director, Department of Administration
Regional Public Safety Communications Center
Port Orange, Florida

Lisa C. Durand
Chief
Johnson County Emergency Communications
Mission, Kansas

Nancy L. Dzoba
Manager, Communications Department
Ft. Lauderdale Police Department
Ft. Lauderdale, Florida

Chris A. Fischer
Director, Communications Department
Valley Communications
Kent, Washington

Barry T. Furey, *Chair*
Executive Director
Knox County Emergency Communications Center
Knoxville, Tennessee

Jenny Hansen
Department of Administration
State of Montana
Helena, Montana

Barry H. Luke
Director, Public Safety
Orange County Fire Rescue
Winter Park, Florida

Paul B. Maison
Homeland Security Coordination Officer
Federal Emergency Management
Washington, DC

Nathan D. McClure
Communications Department
CTA Communications
Lynchburg, Virginia

Richard C. Nowakowski
Manager, Research and Development
Chicago 9-1-1
Chicago, Illinois

Nancy A. Pollock
Executive Director
Metropolitan 9-1-1 Board
St. Paul, Minnesota

Gregory T. Riddle
Executive Director, Department of Administration
West Suburban Consolidated Dispatch Center
River Forest, Illinois

Stephen H. Souder
Administrator, Communications Department
Montgomery County Maryland 9-1-1 Emergency
Communications Center
Rockville, Maryland

Marilyn B. Ward
9-1-1 Administrator
Orange County Public Safety Communications
Orlando, Florida

Don Whitney
Manager, Strategic Market Relationships
Motorola
Schaumburg, Illinois

Introduction to APCO

The Association of Public-Safety Communications Officials (APCO) International is the world's oldest and largest not-for-profit professional organization dedicated to the enhancement of public safety communications. With more than 15,000 members around the world, APCO International exists to serve the people who manage, operate, maintain, and supply the communications systems used to safeguard the lives and property of citizens everywhere.

APCO's mission reflects the importance of the organization and its breadth of activities as they relate to membership needs:

- Foster the development and progress of the art of public safety communications by means of research, planning, training and education;
- Promote cooperation between towns, cities, counties, states, and federal public safety agencies in the area of communications;
- Represent its members before communications regulatory agencies and policy-making bodies as may be appropriate; and through its efforts strive toward the end that the safety of human life, the protection of property and the civic welfare are benefited to the utmost degree; and
- Aid and assist in the rapid and accurate collection, exchange and dissemination of information relating to emergencies and other vital public safety functions.

APCO's Homeland Security Initiatives

The APCO Homeland Security Task Force

The role of public safety communicators became much more evident following the terrorist attacks of September 11th. Often the "first" first responder to emergencies and security issues, public safety communicators serve a crucial role in ensuring the security of the communities they serve and the country at large. With the possibility of chemical, biological or other weapons of mass destruction attacks against American cities, public safety communicators are rising to this challenge by preparing their facilities, staffs and systems to address previously unthinkable events. This critical effort requires the support of a broad coalition of policy makers, legislators, technology vendors, and the public.

APCO International is assisting its members in addressing these new challenges through its own Homeland Security activities and planning efforts. The organization's Homeland Security-directed efforts began with the creation of a Homeland Security Task Force on February 24, 2002. The goals of the task force were five-fold:

1. **Solicit further input from APCO members regarding perceived homeland security issues, threats, and readiness.**

   The task force recognized that significant input is needed from a wide range of APCO members in order to fully define and identify key issues. Feedback from members in all sectors of APCO membership and from a variety of agencies and organizations, large and small, is required to paint a complete picture of the problems, as well as to identify a comprehensive list of potential solutions.

2. **Build a comprehensive list of "best practices" utilizing the APCO White Paper as a springboard for discussion.**

   APCO is the demonstrated leader in matters affecting public safety communications, and our membership has come to rely upon the association as a source of expert advice. APCO is therefore committed to providing the resource tools, guidance, and best practices to help public safety communicators respond to Homeland Security concerns.

3. **Encourage partnerships with other organizations that share common Homeland Security goals.**

   APCO recognizes that it cannot stand alone on the issue of domestic preparedness. Incoming President Thera Bradshaw has emphasized the need for APCO to reach out and partner with other professional organizations, and nowhere is this strategy more important than in matters of Homeland Security. APCO is proactively building bridges with other agencies that share our goals, and is gaining support for meaningful improvements in communications that directly benefit all branches of public safety, as well as the citizens we protect.

4. **Work closely with membership and APCO Institute to identify related training needs and develop course and support material that addresses these specific needs.**

   In order to respond to any emergency, it is imperative for first responders to be adequately trained. Telecommunications personnel have been deemed the "first" first responders, making them the most critical link in the receipt and dispatch of information that is vital to the safety of the entire community. The threat of terrorism has brought with it new challenges and concerns that must be addressed through training. Administrators must also receive training in order to provide the guidance and additional planning skills required to address the issue of Homeland Security at the local level. The APCO Institute will provide this new training.

5. **Increase awareness of Homeland Security through APCO's magazine, *Public Safety*, APCO's web site, and other publications and events.**

   As the voice of public safety communicators, APCO has a duty to share the best practices, lessons learned, and other relevant information with the public safety community at large through as many communication mediums as possible.

APCO's Homeland Security Summit

On June 5th, 2002, APCO International convened a Summit in Washington, DC that brought together legislators, federal officials, state and local representative organizations, and APCO members to begin designing a long-term homeland security strategy for public safety communicators.

Key decision-makers from Congress and the Administration underscored to Summit attendees the importance of the public safety community in ensuring our nation's preparedness against disaster and massive-scale attacks, and the need for public safety officials and decision-makers at all levels to work together to address communications infrastructure needs. Four breakout sessions at the Summit were used to explore these issues in further detail. The following topics were addressed as part of these individual breakout sessions: interoperability and spectrum; security and redundancy; location technology; and funding and state planning.

Representatives from government, public safety agencies, and industry agreed to share their experiences and insights as members of moderated breakout session panels in order to provide guidance to the discussions and, more broadly, to help frame the APCO Homeland Security planning effort as it moves forward.

APCO's Homeland Security White Paper

The terrorist events of September 11, 2001 have impacted the American way of life in many ways, from intensely personal traumas at an individual level to large-scale system traumas. A common change at all levels is the realization that we are now living in an era of "perpetual anticipation." It is clear that at the local level, no need is arguably more important than to improve the communications infrastructure of public safety communications – the precise province of APCO.

The purpose of this white paper is to begin a process that leads to dramatically improving our Homeland Security by improving our public safety communications infrastructure, including the equipment, the procedures, and the training of public safety professionals throughout the U.S. But this white paper is only the "beginning of a process," because the road to dramatically improving our nation's public safety communications capability is a long one that will require knowledge and input from many participants. It will also require significant funding to upgrade and prepare our current public safety infrastructure. To paraphrase Winston Churchill at the start of World War II, we could say that with this white paper, "We are not at the end, nor at the beginning of the end, but we are at the end of the beginning."

The primary goal of this white paper is to identify the current Homeland Security challenges faced by public safety communicators and to highlight some of the activities undertaken by APCO members to meet these challenges. This white paper is meant to create dialogue out of which an APCO Homeland Security guidance document can be formulated. To create this guidance document, APCO International is implementing mechanisms for explicitly gathering input from all disciplines in the public safety community on how they are meeting the challenges of Homeland Security. Together, we need to converge on a set of priorities for improving public safety communications and get the necessary federal, state and local support to have those priorities met.

Public safety organizations and their memberships all have different communications needs and funding requirements. The APCO Homeland Security guidance document will obtain input from all members of this community in formal and informal ways. For example, an online questionnaire will be made available on the APCO International web site to gather input on priority needs and funding required to meet these needs. Special meetings will be held in "town meeting" format, the first occurring at the APCO Conference & Expo, to hear directly from all branches of public safety. Information about best practices, training, and funding opportunities will be posted on the APCO web site. In addition, the APCO Homeland Security Task Force will issue a monthly release about Homeland Security activities in the APCO *Public Safety* magazine. The task force is also considering establishing subcommittees to delve deeper into areas of members' concern.

This white paper is just the beginning of a process that will be ongoing for some years as public safety communicators do their part to ramp up our nation's Homeland Security.

White Paper Topics

Previous discussions of Homeland Security by APCO task forces have concluded that the following six broad topics encompass most of the needs identified following the September 11th events:

- **Radio Spectrum**: having sufficient spectrum for unfettered and high-quality reliable communications in emergency situations.
- **Interoperability**: getting the necessary communications technologies and systems in place so that different public safety agencies can communicate seamlessly and reliably with each other. Developing the ongoing dialogues with other agencies to allow for joint planning and coordination, which is essential for a coordinated response to any type of attack.
- **Planning**: how to approach planning specific to Homeland Security initiatives.
- **Survivability/Redundancy**: knowing how to plan and having the funding available to build public safety communications systems and communication centers that can withstand a terrorist attack or other significant manmade and natural threats.
- **Security**: instigating processes and procedures to assure that public safety communications systems, centers and staff are protected with substantially increased security to thwart attempts by enemies of the United States to disrupt and destroy our emergency communication capability.
- **Personnel/Training**: providing the necessary training to public safety communications personnel to enable them to plan for any type of terrorist event, to utilize new technology, to be aware of new security systems and procedures, and to deal with the stresses associated with working in an environment characterized by "perpetual anticipation."

The Challenge of Spectrum

Today, more than ever, our nation's public safety agencies must have the tools they need to perform their critical tasks. Appropriate radio spectrum is at or near the top of the list of those essential tools.

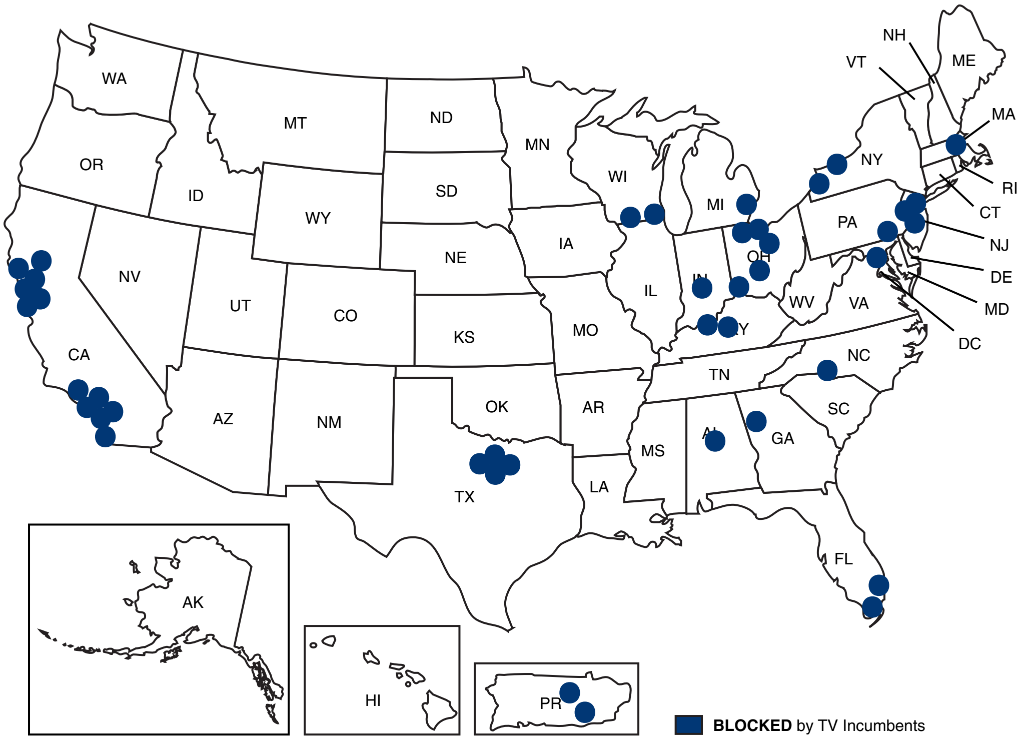
Unfortunately, for far too many years, public safety agencies across the nation have faced a severe shortage of radio spectrum available for their communications systems. The Public Safety Wireless Advisory Committee (PSWAC), a blue-ribbon committee created by National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC), documented these shortages in 1996. The PSWAC report, which was adopted on September 11, 1996, determined that public safety users would require an additional 97.5 MHz of radio spectrum by 2010, and would need approximately 24 MHz within five years of the report. Unfortunately, exactly five years later, on September 11, 2001, that 24 MHz was still not available for nationwide public safety use.

The lack of sufficient radio spectrum for public safety has several significant consequences. In many metropolitan and other densely populated areas, public safety agencies face dangerous congestion on their radio systems. In some instances, public safety agencies operate with hundreds of users per channel, far more than is safe under "normal" day-to-day circumstances, let alone major emergencies. Demand for channel capacity has been increasing with population growth and density. Now, with new Homeland Security responsibilities being placed on public safety personnel, there will be even greater demand for public safety spectrum. Inadequate spectrum also prevents public safety agencies from implementing new communications tools, such as wide-area mobile data systems that can provide law enforcement officers, firefighters, and EMS technicians with a wealth of critical on-scene data. This includes not only high-speed text delivery (such as criminal background information), but also, with sufficient spectrum, high resolution images such as mug shots, fingerprints, and building diagrams. While the FCC recently allocated spectrum in the 4.9 GHz band for certain public safety data and video functions, use of that band will be limited to relatively short distance transmissions. The 4.9 GHz band is not expected to provide a spectrum home for wide-area, mobile data systems.

The lack of spectrum also has a direct and significant impact on interoperability. All too often, public safety personnel from different agencies responding to the same emergency cannot communicate with each other, because they operate on incompatible, non-interoperable radio systems. The lack of interoperability is generally the result of different agencies being forced to operate on different radio frequency bands. The most effective way to address that problem is to migrate agencies in the same geographic area to common, or at least compatible, radio frequency bands. Unfortunately, that is not possible in many areas as there is not enough spectrum in any one band to accommodate all, or even most, of the public safety users in the region. New allocations, especially if adjacent to an existing public safety spectrum allocation, would greatly enhance interoperability with existing users, while at the same time providing capacity for new, multi-agency, multi-jurisdictional radio operations.

Congress tried to address some of these issues in 1997, when it required the FCC to allocate 24 MHz of spectrum for public safety purposes from the 746-806 MHz band (TV channels 60-69). This was consistent with the 1996 recommendations of the Public Safety Wireless Advisory Committee. The FCC then did its part. It reallocated TV channels 63, 64, 68, and 69, for public safety and adopted rules to promote interoperability among all users of the band and the adjacent 800 MHz public safety bands. Indeed, the Commission allocated approximately 10 percent of the new band for nationwide public safety interoperability, and required that all radios in the new band be capable of operating on the interoperability channels. The Commission also adopted a digital interoperability standard (also known as APCO's Project 25, discussed in more detail later in this paper) for the band, to ensure that digital equipment from different manufacturers would still be interoperable.

However, in most of the nation's largest metropolitan areas, the new spectrum allocated for public safety was not available last September 11th, and will not be available until TV broadcasters on channels 63, 64, 68, and 69 (and in many cases the adjacent channels), release those channels as part of the digital television (DTV) transition. The problem facing public safety is not only that the spectrum is not currently available nationwide, but also that there is no firm date for when the spectrum will become available. The 1997 Balanced Budget Act, which required the FCC to allocate spectrum for public safety, allows incumbent broadcasters to continue operation on TV channels 60-69 until December 31, 2006, or until some uncertain, future date when at least 85 percent of the households in the relevant market have access to DTV signals.



700 MHz Public Safety Spectrum Availability Map provided by Motorola, Inc.
This map represents Land Mobile Radio (LMR) usage availability based on nominal LMR communication parameters. Exact coverage areas must be determined by an engineering study based on local propagation conditions.

The Challenge of Interoperability

Interoperability is the ability of different government agencies or first responders (law enforcement, EMS, fire fighters) to communicate within and across departmental and jurisdictional boundaries. It is recognized by first responders as a key factor in determining the success of any coordinated response and has been the focus of improvement efforts by local, state and federal users since 1989.

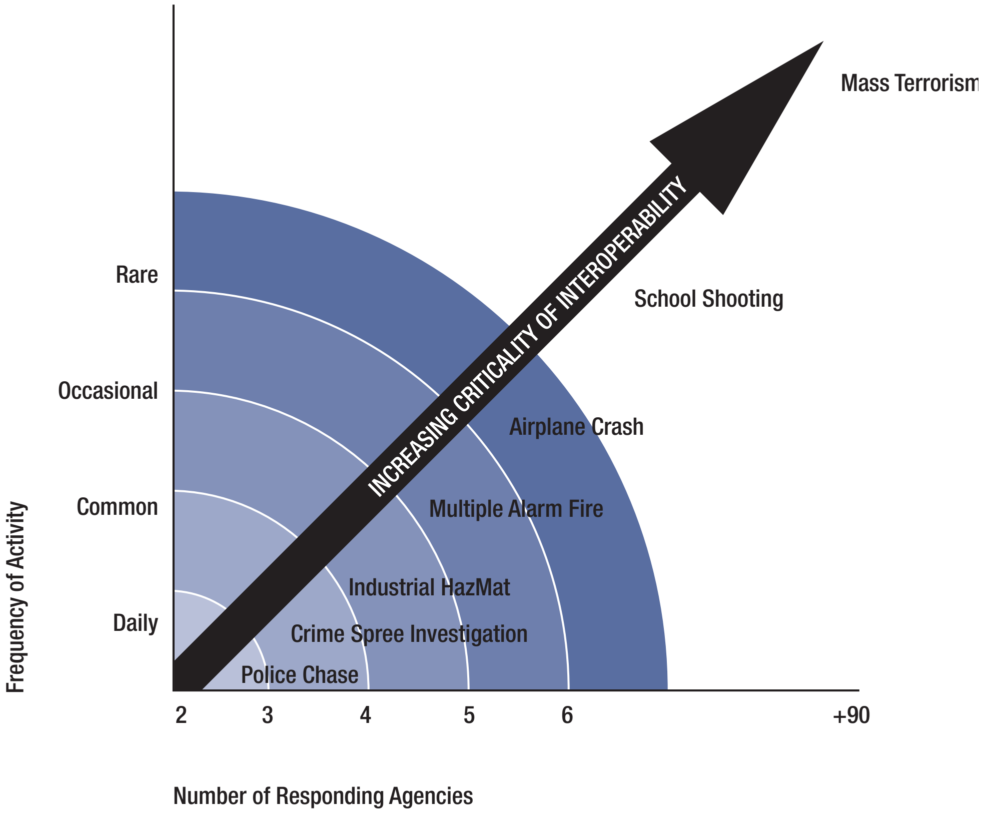
Meeting the interoperability challenge means not only identifying the appropriate communication technology, but also creating communication channels among organizations to allow for preplanning and coordination activities. PSWN, the Public Safety Wireless Network program (a joint initiative of the U.S. Departments of Justice and the Treasury) has identified three types of interoperability:

- **Day-to-day interoperability** covers routine public safety operations, such as responding to a building fire that requires backup from a neighboring fire department, or a vehicle chase that crosses between towns.

- **Mutual aid interoperability** supports a joint and immediate response to catastrophic accidents, large-scale incidents and natural disasters. It supports tactical communications in response to airplane crashes, bombings, forest fires, earthquakes, hurricanes and similar events that occur without warning.
- **Task force interoperability** supports local, state, and federal agencies collaborating for an extended period of time to address a particular problem. For example, a task force might lead extended recovery operations, provide security for major events, or respond to prolonged criminal activity. These are activities that are planned in advance.

APCO supports the PSWN recommendations, which are similar to the Public Safety Wireless Advisory Committee 1996 report definitions.

The technical challenges of interoperability have developed as, over the years, separate government entities deployed systems on different bands and technology protocols. The tendency is for government management and budgets to be segmented along convenient geographic and organizational boundaries. It takes energy and deliberate planning for different agencies to cross over their geographic, jurisdictional and organizational boundaries and work together towards creating an interoperable communication system. Clearly, the less time responders need to spend solving the "how do I talk to the person next to me" problem during a major event, the more they can focus on the dangerous, time critical tasks at hand.



There are essentially six methods to achieve interoperability:

1. **Swap Radios**

   The simplest and most basic level of interoperability is to physically exchange radios with other agencies involved in an event. However, it is impractical for every agency to have extra radios on hand for each member of every other possible agency that could appear on-scene, especially for larger scale events.

2. **Talkaround**

   Talkaround provides interoperability where multiple radio users talk radio-to-radio on the same transmit and receive frequency, in the conventional mode. In this situation, communications are tightly bound by the air interface: the same frequency is required and transmissions are digital-to-digital or analog-to-analog, not analog-to-digital.

3. **Mutual Aid Channels**

   With mutual aid channels, responding radios talk via designated simplex frequencies similar to talkaround or dedicated repeaters, which extend their communications range and allow connection to a console dispatcher. This requires agencies to create a channel plan and to program channels into their radios in advance of an event. As was pointed out earlier with regard to interoperability, preplanning and communication among agencies is just as important as technology.

4. **Gateway/console patch**

   A gateway or console patch is a way of connecting disparate systems with the possibility of different frequency bands. One major drawback for using a gateway or console patch during an unplanned event is that there must be overlapping coverage from the respondent's systems for the gateway to be effective. To get around the requirement for overlapping coverage areas, some gateways are set-up to be transportable. This allows responders from different system types to talk to each other but does have a necessary delay to allow a technician at the scene to set up the relay.

5. **System-specific roaming**

   The response of city and county responders at the Pentagon area last September 11th provides an example of the system-specific roaming method of interoperability. One entity's radios are programmed to work on the other's infrastructure within a set of pre-planned channels or talkgroups. The multiple infrastructure networks provide coverage over large areas without any coverage overlap. Since users can roam from one system to the next they may enlist the help of agencies across the entire area at a moment's notice. This method requires pre-planning and system configurations to accommodate the users of the participating systems.

6. **Standards-based shared system**

   The ultimate interoperability solution, which is useful for any scale of event from small to massive, is a standards-based, shared system. In this method all radios built to a standard can talk to each other via the infrastructure, or in the case of the Project 25 Standard equipment, conventional mutual aid and talkaround also.

APCO Project 25

One very important way that APCO has been addressing the interoperability challenge is through APCO's Project 25, a joint effort of U.S. federal, state, and local governments, with support from the U.S. Telecommunications Industry Association (TIA). The Project 25 standard was created to allow the evolving capabilities of digital technologies to be used for interoperability. The standards process is called "APCO Project 25" and the standards themselves, 102 series of detailed technical specifications for digital, land mobile radio communications systems, are called "Project 25."

While technology is an essential part of resolving the interoperability challenge, planning is a critical first step. Effective planning considers the non technology issues before specific solutions are determined. Interoperability does not involve a single product or system approach; rather it is accomplished with a variety of solutions, at the center of which is the first responder. What is an appropriate interoperability solution varies with the operation of the particular government agencies, their funding, their physical location, and other individual circumstances. There are many approaches to achieving interoperability, but all should be based upon planning for the needs of the responders.

The Challenge of Planning

After the events of September 11th, many communication centers moved quickly to update their emergency response plans, both at the agency and regional level. They found that those emergency management programs that had been "on hold" or scheduled for long term development were now pushed to the top of the priority list. The pressure was on to assure the public that public safety communicators were prepared to answer the call in any situation – regardless of how remote a possibility. At the same time, elected officials wanted assurances that their communication centers could handle responding to new threats.

Public safety agencies and communication centers generally have a firm foundation on which to build Homeland Security policies and procedures: their Y2K or mutual aid disaster plans. In one instance familiar to the APCO Homeland Security Task Force, the Office of Emergency Communications (OEMC) for a major metropolitan APCO chapter city was able to utilize its Y2K plan as a springboard to talk with and revive those plans with city, county, state, federal agencies, and public utilities. But planning for Homeland Security requires that new aspects be taken into consideration. It is important to develop a risk assessment of the area served by the communication center and, in doing so, think "regionally" and determine risks present outside of the immediate area. For one communication center, there was a nuclear power plant within 90 miles of their county and in the event of a major catastrophe, they would have been called to assist. Their prior emergency response plans had not incorporated any nuclear event planning.

It is also important to realize that a major aspect of a terrorism related event will be how to provide necessary information to the public, to reassure them and keep them from panic. Call centers must have adequate plans for unprecedented 9-1-1 call volumes. APCO members have already developed "system overload" plans that change how calls are handled. This also means considering how to plan for implementing a three digit number like 3-1-1 to accept some of the calls. Most recently, 3-1-1 was an alternate number used to process thousands of calls regarding "white powder" when the nation was under threat from anthrax.

Documenting response plans and making sure that they provide appropriate direction for a communication center is important. Many times plans and policies are written for the field and do not address the communication center with enough specificity.

Knowing who should be involved in a response plan is extremely important. Certain states have set up regional terrorism task forces to address the needs of each region. These task forces are made up of representatives from local, state and federal law enforcement, fire, emergency management, medical and health professionals, transportation representatives, and providers of other critical needs such as power companies and telephone providers, including wireless carriers. Creating these types of task forces has opened a vital flow of information between diverse agencies that did little joint planning in the past.

All would agree that a plan for responding to terrorist events should include sections on how to address:

- Interoperability requirements
- Capability of the communications system
- Future system upgrades and expansions
- Incident command escalation / procedures
- Logistics and coordination with critical infrastructure
- Funding sources

In addition, the plans should identify:

- Communication planning team
- Representatives from each partnering agency or jurisdiction (including your neighbors' neighbors)
- Mutual aid agreements
- Critical information, critical resources
- Response procedures
- Roles and responsibilities

Another aspect of emergency planning that is often overlooked is that of staffing. Do plans reflect an accurate picture of the normal staffing levels, or do they require additional telecommunicators to operate effectively? If more personnel are required, how quickly can they be summoned? What can be done to reduce the anxiety level of dispatchers and call takers who may have family or loved ones who are exposed to the threat? Effective planning must consider the human issues involved.

Most important for creating a Homeland Security focused emergency response plan is to realize that many of the "solutions" for various acts of terrorism have not yet been invented. Being from public safety agencies, APCO members are used to implementing procedures that were developed or tested by other agencies. One of the changes in planning for Homeland Security is to think "out of the box." To do so, managers have to allocate sufficient time to plan and prepare for an event with which no one is familiar.

Do Your Plans Work?

Table top and field drills are extremely important in Homeland Security planning as they force operational level participants from all areas to be involved, thereby providing a “reality check” on the procedures being proposed. It is not unlikely that some of the procedures proposed to respond to a terrorist event will not work as initially conceived. It is better to find that out as part of a drill. Drills should include the use of all systems involved so that dispatchers and field units know how to properly use the equipment in an actual emergency. Some APCO members have participated in a Weapons of Mass Destruction exercise in which there was a simulated release of a chemical or biological agent. Response agencies, particularly the fire service, have long recognized the importance of hands-on training. Simulation can provide similar benefits for communication centers, especially when it comes to assessing the capacity to carry out assigned activities with the normally available resources and staffing. Lessons learned from such an exercise allows a city to fine-tune its response capabilities.

Testing plans through drills also identifies any existing gaps and ensures familiarity with critical partners. It reinforces the roles and responsibilities of members within an organization and in partner organizations. It keeps specific skill sets honed. Plans that do not incorporate regularly scheduled drills minimize their value.

Access to New Technology

Lack of equipment or updated equipment has been an ongoing issue for many public safety communicators. At a time of national threat, technology that has been solely created for government use should be shared among the nations’ first responders. Funding to pursue new technologies like software-defined radios should be provided. As part of their ongoing planning, public safety communicators should identify and reach out to known research centers and labs for information on the newest technology. This is another example of the partnerships that must be built in order to deliver effective solutions to the issues involved in Homeland Security.

The Challenge of Survivability & Redundancy Planning

Recent events have forced all entities - government, non-profits, small businesses and industry – to closely examine how secure they are in their operations and how they would respond to a major emergency. Incidents of any size require contingency planning to ensure that networks and building infrastructures can survive potential disruption or failure. Consideration must be given to systems that may be site-specific – such as utilities and heating, ventilating, and air conditioning – as well as larger area infrastructures such as the public switched telephone network (PSTN) and wireless networks.

In assessing their level of readiness, agencies should involve local utilities and telephone providers, including wireless carriers. Critical systems require both redundancy and route diversity, and these providers must be involved in order to get a clear picture of the current state of readiness. If at any point circuits converge on the same telephone pole or in the same manhole, they cannot be considered as being truly diverse.

By identifying, planning for, and implementing “back-up” or redundant systems, agencies increase the effectiveness of their operations during times of uncertainty or massive attack. This is particularly important for ensuring the continuity of 9-1-1 service. Protection of 9-1-1 service might take the form of: system diversity, to the individual circuit diversity level; participation in the Telecommunications Service Priority (TSP) program for service restoration; backup communications and notification systems; and alternate operational locations. Improvements made as a result of domestic preparedness planning have the secondary benefit of providing more robust and reliable systems and processes to our communities on a daily basis.

Several years ago the federal government instituted the TSP program to give priority to provisioning and restoring telecommunications facilities that have been identified as vital to national security or emergency preparedness. This is a tariffed product that is available from the traditional telephone service providers. Following the events of September 11th, U.S. government officials have asked the wireless telephone service providers to offer a method by which emergency responders could be given priority access to the wireless telephone network. This would allow authorized emergency responders' wireless phones to access the network before any other wireless phones are given access. The wireless telephone infrastructure has this capability in most cases, but it has never been utilized by any of the major providers. Local emergency responders should monitor this situation and consider taking advantage of it, if the federal government is successful. Local units of government may also wish to pursue this with the carrier(s) that they contract with for wireless service.

The federal government has already developed a similar program for the wireline telephone network. The program called Government Emergency Telecommunications Service (GETS) gives authorized users priority in call routing. This does not provide a way to get dial tone in a congested network, but it does help ensure call completion once dial tone is obtained. It is more effective in routing calls into a congested network as opposed to placing calls from within the congested network. The program is open to local government officials and requires an application process to be completed.

Redundancy planning for 9-1-1 networks should address:

- Continuation of the operation of the 9-1-1 emergency telephone network;
- Preparation of alternate means of 9-1-1 emergency call completion in the event of system failures;
- Mitigation of service disruption;
- Rapid restoration of any service interruptions; and
- Ensuring public confidence in the 9-1-1 emergency system as a reliable means of summoning assistance.

A metropolitan 9-1-1 Board from one APCO task force member's locality, in cooperation with a vendor and the state government, created and implemented a metro area PSAP Communications Plan that establishes a means of communicating the system-wide incident to all PSAPs in a rapid manner, providing consistent information to each PSAP and, when necessary, to the media for dissemination to the public. If normal means of communicating outage problems to the PSAPs are disrupted, an alternate means of communicating via the state's Criminal Justice Information Network (CJIN) can be employed. A service-affecting problem may be called to the attention of the vendor in one of three ways. Either the vendor's Network Operations Center (NOC), a local exchange carrier NOC, or the PSAP itself may notify 9-1-1 repair that they are experiencing a service disruption. 9-1-1 repair calls the on-duty Sergeant who will initiate a message via the CJIN. The message uses a preprogrammed "all metro area PSAP" group list and transmits the message via data circuits to all PSAPs simultaneously. If the CJIN terminal is not operating at the identified county level, the city's Emergency Communication Center will act as a back-up center. If the CJIN network is not operating, broadcast fax service and individual telephone calls will be utilized. This metro area PSAP Communications Plan is exercised at least twice per year.

While this system illustrates a possible model for other PSAPs to follow, the ability to implement such back-up systems and plans does require the necessary funding to ensure 1) creation/purchase of necessary equipment to ensure redundancy; 2) education and training for employees to ensure familiarity with contingency and security procedures; 3) coordination with local and regional entities involved in emergency response; and 4) continual review to ensure plans are up-to-date and effective with potential area risks.

It must be remembered that attacks against the telephone system can come in many ways. Destruction of cables and switch gear, disabling critical facilities through chemical or biological means, hacking of software, and intentionally overloading circuits are all possibilities. Each of these scenarios must be adequately addressed in order to call a plan complete. Additionally, since many PSAPs bear responsibility for public warning and notification of major emergencies, plans should also address means of maintaining the flow of reliable information to the media during critical failures.

Computer Systems

Not only is 9-1-1 service essential, but the physical security of the 9-1-1 Center and radio transmitter sites should be planned for, as well as the protection of the methods used to transmit and store information. In addition to the computer-aided dispatch systems found in many PSAPs, current radio and telephone systems are also heavily reliant upon computers. Protection against unauthorized access of these systems must also be planned for.

Ensuring the security of computer networks, in particular, is critical to the continued operation of communications networks. The ability to provide computer-assisted dispatching and the dissemination of incident-specific information to appropriate public health/emergency response agencies and the general public (e.g., poison control information, evacuation routes) is normally dependent upon these systems. As a means to this end, PSAPs are being encouraged to build in contingency planning at several levels to help protect their systems from total outage or failure scenarios.

Some questions PSAPs may want to consider when creating the computer system component of their contingency plan:

- What points of access exist on your current computer network? What is their purpose?
- How do you detect that your network security has been compromised?
- What type of countermeasures should you put in place? How are they put in place?
- What are the protective measures necessary for wireline and wireless access points to IT systems?
- How often are these measures checked or updated?

Radio Systems

Radio communication is the lifeline of the first responder. It is the mechanism most routinely used to dispatch calls, and to summon additional assistance, when required. Perhaps no other tool is more relied upon to ensure the safety of officers, firefighters, and paramedics in the field. Any disruption in radio communications – whether it is accidental or intentional – can severely compromise this safety.

It is therefore critical that the security of radio systems be assured so that they remain available to deal with even the most severe incidents. Obviously, equipment contained within the dispatch center will be afforded the same protective measures described elsewhere in this document. However, many agencies rely heavily on remote repeater and satellite receiver sites. In many cases, these are located in secluded areas, or on private property such as high-rise buildings. This further complicates security.

When assessing the reliability of remote radio facilities, the following should be considered:

- Is a suitable fence or other barriers in place?
- How is entrance gained? How many persons have access?
- Is the area well lighted?
- Is the facility alarmed and monitored?
- Are routine patrols assigned to verify security?
- Is there standby power with independent fuel? How long will it run at full load?
- Are the links from this facility to the system redundant, i.e., hot standby microwave or diversely routed T-1?
- What are the ramifications if this facility were disabled?
- Is the facility adequately protected from traditional hazards such as wind, fire, and lightning?

In addition to providing physical protection against threats, radio communications should also be guarded against unauthorized use and hacking. Where radio systems utilize programming, such as 800 MHz trunking, strict controls must be instituted to limit the distribution of programming codes. Unfortunately, in this day and age, information concerning public safety radios can be found, even on the Internet.

Organizations should also assess their radio systems for security of transmissions. With the proliferation of scanners, unless digital encryption is utilized, information transmitted over public safety radio systems should be considered "public knowledge".

The Challenge of Security Planning

Under Homeland Security, security is not assured simply by providing a lock and key. In today's modern world, threats against security are diverse. They include the potential for a biological or chemical attack, as well as intentional hacking of computer systems. Security planning should review building and system access points, protection against explosive devices, training of staff on computer and personal security, review of procedures for contractors accessing the facility and/or essential systems, and security of voice and data content.

A first step in the process of securing a facility is a "threat analysis." Considerations in a threat analysis involve prevention, detection, response and restoration, at a minimum. Significant communications portions of the threat analysis should consider protection of voice or data communications content. In addition to the protection of the voice and data content in the communications system, evaluation of the control signaling protection in both the wired and wireless elements of the system is important.

Facility security even extends to the facility's parking lot. Security fencing is a practical first line of defense. Certain communication centers have installed additional surveillance cameras around the perimeter of the building. Importance has to be placed on redesigning existing buildings to protect against vehicle bombs.

Even though a level of protection may exist, events of the past year may require a reassessment. For example, one agency reports that entrances to their building had already been monitored and, in some instances, access of personnel recorded prior to September 11th. Now, in this heightened security climate, door card security systems are being used to keep unauthorized people out of the facility. Administrators and managers must ask themselves what actions they have taken to protect their facilities from the expanding list of potential threats. Since the anthrax attacks, has your organization changed the way it receives and screens mail?

Employees need to be trained to understand the function and purpose of the security system and procedures implemented at a facility. Maintaining security should be considered a normal part of their responsibilities, and employees should be trained to understand the ramifications related to policy violations and/or security breaches. Administrators need to undertake an evaluation of their security and readiness to defend against attack, and to assess their ability to provide a response in such situations.

Physical security only touches the very tip of the iceberg in defending against terrorism. Networks and infrastructure are a bigger risk with much greater ramifications. Security controls such as data encryption, biometrics, or passwords should be used as barriers against unauthorized personnel on all systems or networks. The appropriate mechanisms for user authentification and authorization need to be maintained when using network access from inside or outside the organization. The days of posting a "sticky" to your computer screen reminding you of different passwords is gone. Employees should be aware of the means of identification needed to access systems in the facility. There should be consistent policies, procedures, roles, and levels of restricted access to sensitive systems.

Controlled access to sensitive systems by subcontractors and staff is of new importance, too. What do you know about the cleaning crew that comes into your facility? Certain communication centers have included clauses in their subcontractors' contract that requires a background check and that each subcontractor meet a minimum-security clearance level. These security clearance levels have been set at either state or local levels.

The mental toll these new security procedures will take on employees in the facility should not be ignored or forgotten. The "bunker mentality" that is collateral to these types of developments in the fight against terrorism needs to be taken into consideration when planning. A balance should be found between the need to defend against a possible attack and the needs of the employees to feel comfortable in their workplace, not displaced and in imminent danger. Assessment can be done through surveying the employees, getting feedback and allowing discussion. Implementation and training through consistent policies and procedures within the security system should help make the altered environment familiar and habitual. Assigned roles and responsibilities within these policies and procedures will create a more protected environment instead of an uneasy one. Consideration should be given to whether food should be stored and how additional food would be provided to employees who, in the event of an attack, must remain in the communication center for an extended period of time. When federal guidelines are set up for vaccinations, employees working in communication centers should be considered the same as first responders in the field. During an incident, it is likely that communication center employees may come in contact with field units, thus becoming exposed to any virus. Some communication centers are requesting chemical/biological grade respirators to protect their staff.

Overall, policies need to be implemented that address key security topic areas such as security risk management, critical asset identification, physical security, system and network management, authentification and authorization, access control, vulnerability management, incident management, awareness and training, and privacy. The intent of each policy must be reflected in the standards, procedures, practices, training, and security architectures that implement it. Management must consider information security a normal part of their responsibility, consequently assigning clearly defined security roles and responsibilities to employees and ensuring adequate resources to fulfill these responsibilities.

An aspect of security planning should also be a plan for building evacuation. As part of that a communication center should address:

- Under which situations is an evacuation necessary?
- What are plans for continuity of service?
- What are the evacuation routes?
- Where are the assembly areas and what are the procedures for accounting for personnel?
- How do you notify off-duty staff?
- What are the criteria for re-occupying your communication center?

One should also consider if there is a "crash kit" available, in case of immediate evacuation, that contains minimum supplies such as phone numbers, portable radios, master keys, flashlights and extra batteries, and a copy of your emergency response plan. In light of the events at the World Trade Center, the need for a tested evacuation plan is now obvious.

The Challenge of Personnel Training

Some of the most important training that needs to occur to prepare public safety communicators for Homeland Security starts with the dispatchers and call takers.

It is critical that these individuals receive training in critical analysis of information to be able to spot an escalating incident. Dispatchers need additional information since they might be put in the role of helping to locate triage and evacuation areas.

Some of the identified new training areas:

- How to handle biological and chemical incidents (how to understand the signs, symptoms and progression of these attacks)
- Awareness of secondary exposure and explosives
- Proper questions to ask when taking a call related to suspicious substances or incidents

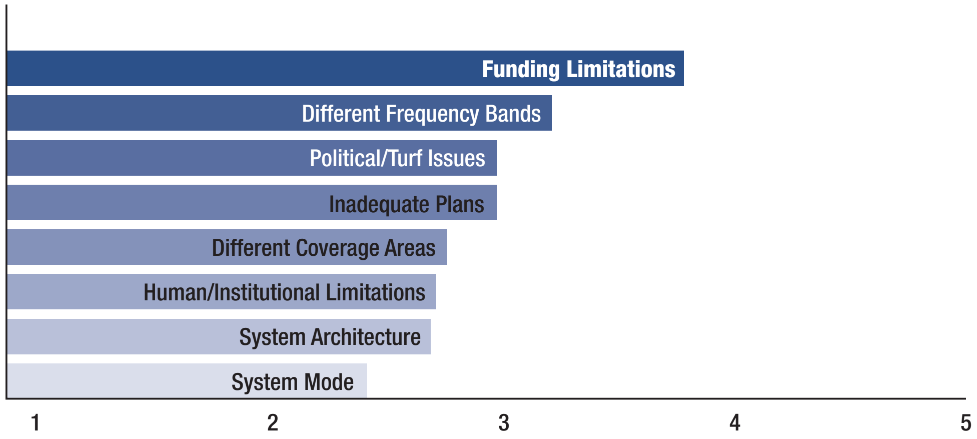
Additional training topics for all public safety communicators:

- Facility security
- Radio systems training
- Incident command training
- How to obtain grant funding

Training needs to be created in multiple platforms and methodologies. What works for a large communication center does not necessarily work for a smaller one. With time of the essence, APCO is proud to have online learning modules already available through the APCO Institute and is working hard to provide training in some of the topic areas identified by our membership.

Conclusion

Devising an effective approach to solving the issues addressed in this white paper is a much greater task than APCO should attempt on its own. Consequently, we are reaching out to all stakeholders in the public safety community to gather lessons learned, guidance documents, advice, and best practices to frame further guidance documents specific to the six issue areas described herein. As we have all learned throughout the course of the past year, emergency preparedness and planning is a global issue that requires thorough communication and coordination between all cities and counties, regardless of size. We also realize that in order to be truly effective in our preparedness goals, we must provide proactive rather than reactive solutions.



[1=Not a Problem to 5=Major Problem]

Understanding this, APCO intends to partner with local, state, and federal public safety organizations in the development of cooperative projects and coordinated efforts intended to address the infrastructure issues most critical to public safety communicators. Further, we intend to keep our focus on the factor underpinning all of our planning efforts – funding. It is acknowledged that public safety communications has traditionally not received a proportionate share of grant monies and that independent PSAPs, in particular, often fall outside of narrow funding guidelines. We want our membership and our partners to realize that we have listened to their concerns and experiences and recognize how crucial the funding issue is to each and every one of the considerations explored in this paper and our preparedness efforts to date. The ability to understand, asses the situation, and communicate effectively is paramount, but progress cannot be achieved without access to the funding required to reach the necessary levels of preparedness being requested by the highest levels of the Administration.

As the leading voice on public safety communications issues, APCO International looks forward to working with public safety agencies and governments throughout the world as we further explore the issues raised in this white paper. While the focus of this paper has been driven by the impact of September 11th on public safety communications in the United States, APCO International acknowledges that these problems and solutions exist worldwide and that the challenge is broader than the events of even that single day. Many of our international members have first-hand experience with the effects of terrorism, and this experience will be called upon in defining best practices. Our efforts to date, and the efforts of all of our partners moving forward, are critical to ensuring the protection of the public and our membership.

Reference Documents:

1. **PSWN Strategic Plan; Achieving Interoperability Through Cooperation and Coordination**

   Recent events such as acts of domestic terrorism, such as Oklahoma City, have highlighted the importance of coordinated interactions among public safety agencies from all levels of government. The PSWN Program was formed to promote effective public safety communications and to foster interoperability among local, state and federal communication systems. This plan describes our vision of seamless, coordinated, integrated communication to effectively protect lives and property

   http://www.pswn.gov/strategic_plan_1_5_99.htm#plan

2. **National Institute of Justice Research in Brief; Wireless Communications and Interoperability Among State and Local Law Enforcement Agencies**

   This brief discusses a 1997 survey designed to provide quantitative data from state and local law enforcement agencies nationwide on their current and planned use of communications equipment and services and their experience with interoperability. They found that interoperability is common, but there are serious obstacles such as funding limitations and frequency incompatibility, which make it difficult for agencies to communicate beyond their local network.

   http://www.ncjrs.org/pdffiles1/168945.pdf

3. **Understanding Wireless Communications in Public Safety; A Guidebook to Technology, Issues, Planning, and Management**

   The National Law Enforcement and Corrections Technology Center (NLECTC) system was conceived with the idea of helping public safety personnel understand and use new technology. This guidebook is meant to help unravel the confusing issues, terms and options surrounding wireless communications, particularly as it involves commercially available communications services. The guidebook covers 1) planning and managing a strategic project; 2) wireless communications technology; 3) wireless communications issues; and 4) wireless communications options.

   http://www.nlectc.org/pdffiles/wirelesspdf.pdf

4. **Analysis of Response to Sept. 11 Pentagon Attack Shows Value of Preparedness, Challenges to be Overcome; Arlington County Creating Emergency Preparedness Blueprint from 9/11 After-Action Report Recommendations and First-hand Experience**

   This analysis of the response by personnel in Arlington to the 9/11 attacks on the Pentagon outlined five best practices and five key challenges for other response teams to consider and follow.

   http://www.co.arlington.va.us/NewsReleases/Scripts/ViewDetail.asp?Index=843

5. **Common Sense Guide for Senior Managers; Top Ten Recommended Information Security Practices – First Edition, July 2002**

   Surveys indicate that problems with information assurance and computer security are far from resolved, and companies altogether lose billion dollars of revenue due to security breaches. The Internet Security Alliance aims to identify and standardize best practices in Internet security and information survivability. In its efforts to improve information security and sharing, ISA developed the Best Practices Working Group, which has identified the 10 of highest priority and recommended security practices as a place to start for today's operational systems.

   http://www.isalliance.org/news/BestPractices.pdf

6. **PSWN Program; Standards and Technology**

   Under Standards, the program contains guides and reports designed to help the public safety community understand the fundamentals of the standards development process and the effect these standards have on public safety interoperability. Under technology, the program contains studies and reports that examine the wireless technologies present in the marketplace and how they relate to public safety interoperability.

   http://www.pswn.gov/library/lib_standards.htm

7. **NFPA Standard 1221**

   This standard describes the installation, maintenance, and use of public fire emergency services department communications systems, those used to receive emergency and non-emergency requests for service calls from the public and to re-transmit those alarms to emergency response agencies, fire companies, and other agencies.

   http://www.nfpa.org/Codes/NFPA_Codes_and_Standards/List_of_NFPA_documents/NFPA_1221.asp

The Association of Public-Safety Communications Officials
World Headquarters
351 N. Williamson Blvd.
Daytona Beach, FL 32114-1112
www.apco911.org

August 2002